Western New England Law Review

Volume 7 7 (1984-1985)
Issue 3

Article 10

1-1-1985

PERSONAL PRIVACY AND THE "1984" SYNDROME

Toby Solomon

PERSONAL PRIVACY AND THE "1984" SYNDROME†

TOBY SOLOMON*

TABLE OF CONTENTS

* Associate, Stern, Steiger, Croland & Conway, Paramus, New Jersey; B.S. Ohio State University; M.A. Columbia University; J.D. Seton Hall University.

> As every man goes through life he fills in a number of forms for the record, each containing a number of questions. . . . There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized as rubber bands, buses, trains and even people would lose the ability to move. . . . They are not visible, they are not material, but every man is constantly aware of their existence. . . . Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads.[1]

I. IMPACT OF COMPUTERS ON SOCIETY

A. *Introduction*

1. The Computer-Created Dossier

It is difficult to ignore the impact that computers have had on informational relationships and personal privacy. The compilation, recordation, and analysis of vast amounts of information can be efficiently accomplished with the advance of computer technology.[2] Society seems to be entering a new period in which information is a significant factor. A generation ago business and government possessed substantially less information about individuals. Decisions concerning government benefits, extension of credit, or insurance were once made on a personal level. Records were simply maintained in manila folders and filed in a single office. They were rarely circulated beyond the place in which they were compiled.[3]

Most Americans are currently unaware of the extent to which federal agencies and private companies use computers to collect, store, and exchange information about the many activities of individuals.[4] Every application for a credit card, loan, insurance policy, medical care, employment, education, or government services is evaluated according to the information recorded in the files of one or more organizations.[5] The average American may be the subject of between ten

---

1. A. SOLZHENITSYN, CANCER WARD 189 (1968).

2. Gobert, *Accommodating Patient Rights and Computerized Mental Health Systems*, 54 N.C.L. REV. 153 (1975-76).

3. PRIVACY PROTECTION STUDY COMM., PERSONAL PRIVACY IN AN INFORMATION SOCIETY, 3-4 (1977) (hereinafter cited as PRIVACY COMMISSION REPORT).

4. *Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcommittee on Constitutional Rights of the Committee on the Judiciary United States Senate*, 92d Cong., 1st Sess. 9 (February, March 1971) (hereinafter cited as *Hearings, Federal Data Banks*).

5. Plishner, *"It's None of Your Business." Or Is It? California Addresses the Computer Age*, 8 RUTGERS COMPUTER & TECH. L. J. 235 (1981).

and twenty individual "dossiers" and as each day goes by that situation worsens.[6] Americans generally dislike the term dossier. The computer data of today, however, is the dossier of tomorrow.[7] The time span covered by each individual dossier presents an additional problem. We are developing the technological capacity to immediately exchange and communicate information, regardless of its quantity.[8] One commentator has observed that "[t]his is a unique characteristic of modern informational society."[9]

2. The Concern for Privacy

The concern for privacy is deeply rooted in American history. This nation was founded by immigrants who traveled from Europe in anticipation of a fresh start.[10] Personal privacy is one of America's most valued rights. Since the Pilgrims landed at Plymouth, Massachusetts, Americans have demanded the right to control the collection of personal information about themselves. The Pilgrims essentially sought privacy when they traveled to America.[11]

Today, computer information and records continue to be stored long after they have served their purpose. Computer technology has virtually created an "information prison" from which one cannot escape.[12] What happens to the individual who wants a new start? Walter Malone, in "Opportunity,"[13] described the plight of such an individual as follows: "Each night I burn the records of the day - at sunrise every soul is born again."[14] If derogatory information is stored and used against a man long after an event, this could never be true. People tend to forget and forgive, computers do not. Further, most of the time the individual has little control or even knowledge over what personal information will be collected. A survey conducted by David

6. *Hearings, Federal Data Banks, supra* note 4, at 9 (statement of A. Miller, professor of law, Univ. of Michigan).

7. Gobert, *supra* note 2, at 153.

8. *Hearings, Federal Data Banks, supra* note 4, at 12 (statement of A. Miller, professor of law, Univ. of Michigan).

9. *Id.*

10. *Hearings, Federal Data Banks, supra* note 4, at 51 (statement of B. Neuborne, staff counsel, Am. Civil Liberties Union).

11. APPROACHES TO PRIVACY AND SECURITY IN COMPUTER SYSTEMS, U.S. DEPT OF COMMERCE, National Bureau of Standards (Sept. 1974)(statement of Hon. B. Ancker-Johnson, Dept. of Commerce)(hereinafter cited as PRIVACY AND SECURITY IN COMPUTER SYSTEMS).

12. *Hearings, Federal Data Banks, supra* note 4 at 52 (statement of B. Neuborne, staff counsel, Am. Civil Liberties Union).

13. *Id.*

14. *Id.*

F. Linowes, former Chairman of the United States Privacy Protection Study Commission of the University of Illinois,[15] indicated that forty-two percent of the 469 agencies responding to the study said that subject individuals are *not* notified[16] of their inclusion in a data bank. Moreover, it was found that virtually all intelligence data fell within this category.[17] Although fifty-three percent of the agencies indicated that an individual may review his file, the right to review is illusory[18] if an individual is not aware of the existence of a file in the first place. Additionally, the information may be used for a purpose other than that for which it was originally collected.[19] Sophisticated retrieval systems render information from computers instantaneously. Computers not only expand the memory of man a trillionfold, they extend enormously his ability to retrieve and integrate with other information and to send it almost anywhere in the world.[20] Centralization of vast quantities of personal information and its potential availability to government officials, employers, police departments, credit companies, and many others, for both legitimate and illegitimate purposes, pose a substantial threat to privacy.[21] As people deal with governmental agencies, private business, large corporations, or institutions, they realize that paper dossiers and computer printouts may contain only half the truth.[22] Further, the computer has the ability to "combine scattered bits of data into a comprehensive personal data."[23] The fallibility of computers poses an additional threat to personal privacy.[24]

Not surprisingly, the National Data Center proposal became a catalyst for the feelings of apprehension generated by the use of computers.[25] Proponents of the idea thought it would:

1. Make more data available for researchers, both inside and outside government;
2. Reduce the unit cost of data;

---

15. D. Linowes, *Research Survey of Privacy and Big Business*, Survey Research Laboratory of the Univ. of Illinois at Urbana-Champaign, (July 27, 1979).

16. *Id.*

17. *Subcomm. on Constitutional Rights of the S. Comm. on the Judiciary, Federal Data Banks and Constitutional Rights*, 93d Cong., 2d Sess. 747 (1974).

18. *Id.*

19. *Id.*

20. *Hearings, Federal Data Banks, supra* note 4, at 2.

21. Gobert, *supra* note 2, at 153.

22. *Hearings, Federal Data Banks, supra* note 4, at 1.

23. Comment, *The Privacy Act of 1974: An Overview and Critique*, 1976 WASH. U.L.Q. 667, 671.

24. *Id.* at 672.

25. A. MILLER, THE ASSAULT ON PRIVACY 57 (1971).

3. Enable larger and more effective samples to be taken;
4. Facilitate the canvassing of a wider range of variables;
5. Reduce duplication in government data collection activities;
6. Promote greater standardization of techniques among the agencies;
7. Make research efforts easier to verify; and
8. Provide a data processing pool for all the agencies handling information.[26]

A fatal error of the proponents of the National Data Center's proposals, however, was their obsession with efficiency and their lack of concern with the problem of privacy. Professor Arthur Miller stated that the apparent victory against the National Data Center is a "Pyrrhic one,"[27] because the failure to establish a data center under a legislative mandate directing the managers to take the steps necessary to protect individual privacy may serve to undermine individual privacy in the long run.[28] It is the intention of each federal agency to develop a data center.[29]

Additionally, the technology of security in this field has not been maintained, or it is just too expensive to be feasible. Errors can occur in the process of data transfer. "The mere collection and retention of sensitive or personal information creates a state of severe psychological insecurity."[30] Some Americans are worried that the existing laws are no longer adequate to protect each individual against the "information power" of government and other organizations.[31] The public's need to know, versus its need for a certain amount of privacy, has created a conflict. Privacy in a society such as ours must be balanced against other needs.

B. *Balance*

Society seeks more and more services from the government as well as from private organizations. Increasingly complex institutional functions, public welfare programs, and large business dealings and law enforcement needs require complex information systems. Individuals have come to expect welfare, social security benefits, unemployment compensation, and guaranteed loans from the government.

26. *Id.*
27. *Id.*
28. *Id.*
29. *Id.* (footnotes omitted).
30. Comment, *Supra*, note 23, at 674.
31. *Hearings, Federal Data Banks, supra* note 4, at 1.

They expect instant credit to enable them to travel anywhere in the world and expect to pay for services, food, and lodging with credit cards. Professor Linowes suggests that "[a]dministrators responsible for furnishing these services must satisfy themselves of a person's eligibility by demanding and getting much personal, often sensitive, information."[32] Computer technology has met these needs by making it possible and practicable for organizations to store, retrieve, and analyze data.

> The very real benefits conferred by information technology may opiate our awareness of the price that may be exacted in terms of personal freedom. . . . [T]he computer is precipitating a realignment in the patterns of societal power and is becoming an increasingly important decision-making tool. . . . As society becomes more and more information oriented, the central issue that emerges to challenge us is how to contain the excesses and channel the benefit of this new form of power.[33]

The boom in record-keeping and the expansion of the personal data services industry has resulted from three sociological factors delineated in 1977 by the United States Privacy Protection Study Commission: (1) The tremendous expansion in the use of credit; (2) the unparalleled mobility of population; and (3) the enormous increase in the work force.[34]

Today information is power. The amount of data that one institution or individual has over another is often directly related to control over that entity. The two major issues involved in the public's "need to know" syndrome involve managing the information explo-

---

32. Linowes, *Must Personal Privacy Die in the Computer Age?* 65 A.B.A. J. 1180,1182 (Aug. 1979).

33. A. Miller, *The Right of Privacy: Data Banks and Dossiers*, published in PRIVACY IN A FREE SOCIETY (Final Report of the Chief Justice Earl Warren Conference on Advocacy in the United States) 72, 83 (1974). *But see* A. WESTIN & M. BAKER, DATABANKS IN A FREE SOCIETY (1972). Based on their field research, the authors perceived that computerized records did not pose a threat to the privacy of American citizens. *Id.* at 341. Their book has been criticized and questions have been raised as to whether there was sufficient evidence to support their position. *See e.g.*, Kane, Book Review, 24 BUFFALO L. REV. 331 (1974-75).

34. Privacy Commission Report, *supra* note 3, at 3-4. The Privacy Protection Study Commission found "imbalance in the relationship between individuals and record-keeping organizations." *Id.* at 6. It recommended three objectives to ensure effective privacy protection: (1) minimizing intrusiveness by balancing what an individual is expected to divulge and what he or she seeks in return; (2) maximizing fairness by delineating the nature and extent of record-keeping operations; and (3) creating legitimate and forceable expectations of confidentiality by law or statute and by reasonable enforcement procedures. *Id.* at 14-15.

sion and the public's demand for greater services. Increased services mean that people must divulge more information about themselves, and consequently they have less privacy.

C. *Need for Privacy*

Perhaps privacy, an ambiguous notion at best, should be examined in relation to existing records and record-keeping practices. It is difficult to formulate a precise definition or even a workable one. Dictionary definitions of privacy speak of seclusion, retirement, and freedom from observation and interruption.[35]

> For any one individual, privacy, as a value, is not absolute or constant; its significance can vary with time, place, age and circumstances. There is even more variability among groups of individuals. As a social value, furthermore privacy can easily collide with others, most notably free speech, freedom of the press, and the public's "right to know."[36]

Privacy, like the concept of happiness, is both elusive and fluid. Yet no one will seriously dispute the fact that a modicum of each is a necessary condition to mental and environmental well being. Conceivably, a society which fails to sufficiently preserve the individual's privacy may experience behavioral patterns such as irritability, mistrust, and hostility.[37] Further, it is commonly believed that personal privacy is essential to an individual's well being in four areas: social, moral, physical, and psychological.[38] Moreover, if citizens become aware that their actions are being monitored they may become less willing to engage in constitutionally protected activities that are expressly allowed and encouraged. In short, we could develop a "record prison psychology" in this country.[39] Dossiers and files do not actually have to be used to repress a people. If the government gives the appearance of repression, that in itself could give a chilling effect to the rights guaranteed by the Constitution.

As recently as a decade ago, people considered Aldous Huxley's *Brave New World*[40] and George Orwell's *1984*[41] to be exaggerated sci-

---

35. WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1804 (1976).

36. U.S. DEP'T OF HEALTH EDUCATION AND WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS 38 (1973) (hereinafter cited as HEW REPORT).

37. *Hearings, Federal Data Banks, supra* note 4, at 74 (statement of Prof. Raymond Katzell).

38. Gordon, *The Interface of Living Systems and Computers: The Legal Issues of Privacy*, 4 COMPUTER/L. J. 877, 886 (1980).

39. *Hearings, Federal Data Banks, supra* note 4, at 10.

40. A. HUXLEY, BRAVE NEW WORLD (1932).

ence fiction.[42] Some Americans believe that we have entered an "Orwellian period." Many Americans do not appreciate the extent of information that modern technology is capable of monitoring, collecting, and storing. The fact is that many Americans are now the subject of a "womb-to-tomb" dossier.[43]

Mr. Justice Brandeis addressed this problem in the 1928 case of *Olmstead v. United States*[44] where he stated:

> Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning, but without understanding.[45]

Previous dictatorships have repressed society with machine guns, tanks, and armies, but repression may come in the form of an Orwellian psychology, with data banks and dossiers. Is not "1984" a state of mind? A dictatorship of data banks and dossiers could be just as chilling on our precious Constitutional protections.

II. COMPUTERIZED MEDICAL RECORDS: A CASE IN POINT

The obvious difficulties encountered in an attempt to assess computer threats to personal privacy are clearly demonstrated in the health care professions. The need to balance an individual's right to privacy and the public's right to medical services is striking. The practice and financing of medicine has changed dramatically in the past decade. "Third party payment"[46] is now the norm rather than the exception. Further, clinical records have been standardized and automated. If the suggestion of some information specialists were followed, everyone would be assigned a birth number for identification.[47]

---

41. G. ORWELL, 1984 (1932).

42. *Hearings, Federal Data Banks, supra* note 4, at 8.

43. *Id.* at 9.

44. 277 U.S. 438 (1928)(holding that the Fourth Amendment did not govern wiretappings).

45. *Id.* at 479 (Brandeis, J., dissenting). *But see* Berger v. New York, 388 U.S. 347 (1967) (holding the Fourth Amendment's protection against unreasonable and warrantless searches and seizures did cover both wiretapping and eavesdropping).

46. *Id.*

47. A. Miller, *supra* note 25, at 4. Using a birth number eliminates much of the existing multiplicity in record-keeping while at the same time expediting the business of society. The wide-spread use and abuse of birth numbers has been contemplated in modern science fiction. For a fictitious description of the possible abuses of birth numbers ("namebers"), see I. LEVIN, THIS PERFECT DAY (1970).

Arguably, there are valuable uses for computerized birth numbers in the medical field. For instance, if a person fell ill away from home, a doctor could use the patient's birth number to retrieve the patient's medical history and drug reactions from a central medical bank.[48]

There are substantial off-setting risks, however, to be considered. Birth numbers could be used as a leash around our necks and make us the subject of monitoring, thus fulfilling the prediction of a "womb-to-tomb" dossier.[49] There is growing public concern that the Social Security number will become a standard universal identifier (SUI). An SUI is a systematically assigned label that, theoretically at least, distinguishes a person from all others.[50] Therefore, medical data poses this efficiency-privacy dilemma in a particularly acute form. For many people medical records are the most sensitive form of personal information. If one questions the fact that the disclosure of personal medical information could affect one's entire future, recall what happened to the 1972 Democratic Party nominee for Vice President, Senator Thomas Eagelton, after it was disclosed that he had sought psychiatric help.

Although a potential threat to an individual's right to privacy, easy access to medical records is vitally important in treatment, research, disease control, the formation of public policy, and in compensating the victim of accident or disease.[51]

Traditional legal principles and doctrines applicable to medical privacy, such as the physician-patient privilege and the common law right to privacy, are inadequate to deal with questions which arise in automated medical data systems.[52] New general principles of protecting informational privacy are equally applicable to medical data systems: there should be no secret data systems; the individual should be able to determine what personal information is recorded; and one should be able to correct any inaccurate information.[53]

The privacy of medical records has not been adequately protected in the United States. Economic and social issues, together with technological advances, have even further eroded the confidential relationship traditionally existing between patient and health care professional. Further, health insurance programs have been accompa-

48. A. Miller, *supra* note 25, at 4.

49. *See supra* note 43 and accompanying text.

50. HEW REPORT, *supra* note 36, at 108-9.

51. Boyer, *Computerized Medical Records and the Right to Privacy: The Emerging Federal Response*, 25 BUFFALO L. REV. 37, 39 (1975).

52. *Id.*

53. *See* HEW REPORT, *infra* note 180 and accompanying text.

nied by ever increasing requests for information from patient health records in substantiating claims for payment. Additionally, there are demands for patient health information for medical care evaluation.

The Hippocratic Oath imposes upon physicians only a *moral* obligation to refrain from the improper disclosure of personal information.[54] Further, even if there is a state law prohibiting disclosure of information in medical records, it is only for the records of physicians, not other health care personnel. In the mental health field the principle of confidentiality between patient and therapist is considered so fundamental that physicians cannot even consult with their professional colleagues about a particular patient's problem unless that patient's consent is first obtained.[55] Disclosure to computer personnel for purposes of coding would, therefore, be a violation of confidentiality.

Computer personnel are not under the same obligations and professional standards as mental health professionals. Therefore, in the case of the therapist, the patient's permission should be obtained before divulging information to computer personnel. The Privacy Protection Study Commission stated:

> The outward flow of medical data . . . has enormous impact on people's lives. It affects decisions on whether they are hired or fired; whether they can secure business licenses and life insurance; whether they are permitted to drive cars; whether they are placed under police surveillance or labelled a security risk; or even whether they can get nominated for and elected to political office.[56]

In addition, the commission advocated the patient's right to inspect and copy his records. This right, however, is not absolute because it might in some situations be unwise to give the patient such information, as opposed to a designated third-party. There is generally agreement with respect to the patient's right to correct inaccurate information. An area of controversy is whether government officials

---

54. 14 ENCYCLOPEDIA AMERICANA 218 (Int'l ed. 1978). The Hippocratic Oath, in relevant part, commands: "Whatever, in connection with my professional practice, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret."

55. Gobert, *supra* note 2, at 166. (quoting AMERICAN MED. ASS'N JUDICIAL COUNCIL OPINIONS AND REPORTS § 9(5)).

56. PRIVACY COMMISSION REPORT, *supra* note 3 at 281 (quoting A. Westin, *Computers, Health Records, and Citizens' Rights* 60 (1976)). The report continues: "The physician-patient relationship is an inherently intrusive one in that the patient who wants and needs medical care must grant the doctor virtually unconstrained discretion to delve into the details of his life and his person." *Id.* at 282.

should have access to medical records.[57]

The American Medical Record Association (AMRA) recognized the need for patient health information in providing a sound basis both for substantiating claims and for the evaluation of medical care.[58] The AMRA, therefore, reaffirmed the patient's right to privacy with regard to his personal medical record.[59] It stated that any release of individually identifiable medical information for any purpose other than patient care must be done only with express informed authorization of the patient or his legal agent.[60] Traditionally, the patient's right to privacy has been protected by requiring his written consent concerning the release of information.[61] This is unrealistic, however, considering the pressures for such release. It is, in fact, a major loophole in privacy enforcement. Financial, legal, administrative, educational, research, and audit requirements are factors that contribute to the complexity of preserving confidentiality.[62] Most patients have little choice in deciding whether to pay a large medical bill or whether to disclose information in order to get reimbursed.

Medical data systems generally have three functions: those used in direct support of clinical care; those that are devoted to statistical research; and those employed in the process of providing payment for medical treatment.[63]

A. *Clinical Care*

Records that are needed for diagnosis and treatment are typically located in different doctor's offices, clinics, laboratories, or hospitals. Most Americans cannot locate all of their personal medical records. It would be a most difficult task to try to obtain all medical records from date of birth to present. The extreme mobility of the American people adds to this difficulty. Most of us recognize that the onus is on us to perform the necessary record-keeping.

Computer systems are an attractive alternative to the present inefficient system. The development of automated patient records, however, has not been widely used.[64] Computers employed in hospi-

57. *Id.* at 298.

58. PRIVACY AND SECURITY IN COMPUTER SYSTEMS, *supra* note 11, at 63 (statement of M. Beard, American Medical Record Ass'n).

59. *Id.*

60. *Id.*

61. *Id.* at 62.

62. PRIVACY AND SECURITY IN COMPUTER SYSTEMS, *supra* note 11, at 62 (statement by Bowden, *The Medical Patient's Right to Privacy*).

63. Boyer, *supra* note 51, at 40.

64. A. WESTIN & M. BAKER, DATA BANKS IN A FREE SOCIETY 204 (1972).

tals and clinics are usually used for administrative functions such as admissions and billing rather than for the actual treatment process. There are primarily two reasons for the current lack of computer utilization. First, medical and health-related personnel are not sufficiently comfortable with the idea of delegating professional responsibilities to computers. Second, medical records are difficult to reduce to machine readable form because a patient's individual medical record is basically a narrative document.[65] Further, the problem of confidentiality may arise with increased computer utilization and doctors fear a loss of control over confidential medical information.

A significant advantage in using computer systems for linking patient records is that the individual's medical history can be accurately stored and retrieved when needed. Greater accuracy in a diagnosis based upon the computer's suggestion is likely to result. The computer affords the ability to compare various treatment plans with their potential results. The unique characteristics and needs of each patient can be compared with the results of similar patients and treatment plans. Clinical computing systems have also been developed to identify patients who would be unusually vulnerable to illness.[66]

If interest continues and costs become feasible, it is likely that clinical records will eventually be computerized. When this occurs, the individual's privacy will be even further eroded. A data center which adequately meets patients' needs will have to be quite extensive and readily accessible over a wide geographic area. To achieve this constant accessibility and flexibility, it will be difficult to maintain the individual's privacy. It would be a difficult task to restrict and monitor the disclosure of such information to authorized personnel with a legitimate need.[67] Further, the economic reality is that using a large scale computer system for one purpose will probably not be feasible. For example, there may be economic pressure to use such a system for billing, statistical, or other research purposes. Many automated personal data systems established primarily for administrative purposes are also used for statistical reporting and research. The Department of Health Education and Welfare suggests: "Since one advantage of computerizing administrative records is the capability thereby acquired for high-speed data retrieval and manipulation, a growing

65. *Id.* A computer system designed to store records in a narrative format would require so much storage space that it would be prohibitively expensive. *Id.* This is even more true of psychiatric records than that of the average medical record. *Id.*

66. Barnett, Keopsell, Nesson, Dorsey & Phillips, *An Automated Medical Record System*, 224 J.A.M.A. 1616, 1620 (1973).

67. Boyer, *supra* note 51, at 46.

number of administrative data systems will be put to such additional uses."[68]

B. *Computers Used for Health Statistics*

In 1967, the National Institute for Mental Health authorized grants for the development of a Multi-State Information System for Psychiatric Records (MSIS).[69] Each participating state has its own facility which uses special forms to collect information about the patient, the problem, the prognosis, the treatment plan, and the recovery process.[70] The data collected is generally stored in computer files. This data can then be used to ascertain the distribution of patients and the types of problems common to various mental health facilities.[71] A state can then allocate specialists and financial resources to institutions when needed. Further, the computer can describe the demographic characteristics of clients receiving mental health services, and administrators can offer better services and programs in the future.[72]

Poorly conceived data collection can result in various injuries to individuals.[73] Any personal data file is a potential source of harm to an individual if it is used outside its appropriate context. Many individuals are under the mistaken impression that the requested data must be provided under penalty of law.[74] That is clearly not correct: "When application forms or other means of collecting personal data for an administrative data system are designed, the mandatory or voluntary character of an individual's response should be made clear."[75]

---

68. HEW REPORT, *supra* note 36 at 78.

> For example, college students applying for government-guaranteed loans in one State have been required to provide the State guarantee agency with data on matters that had no direct relation to its individual entitlement decisions. These data, "for our statistical interest" as their intended use was described to the Committee, include race, marital status, sex, adjusted family income, and student reported average grades received for "past term of full time post-high school study." These data have been used to produce statistical reports for internal agency use, for informal discussions with State legislators and to "run a profile once yearly on . . . schools and . . . lenders to see if there is any odd pattern . . . occurring." On one occasion data in the system also have been used in a study conducted by an outside researcher.

Id. at 79.

69. Curran, Laska, Kaplan & Bank, *Protection of Privacy and Confidentiality*, 182 Sci. 797, 798 (1973).

70. *Id.*

71. Gobert, *supra* note 2, at 157.

72. *Id.*

73. HEW REPORT, *supra* note 36, at 80.

74. Gobert, *supra* note 2, at 50 (footnotes omitted).

75. HEW REPORT, *supra* note 36, at 80.

Additionally, all personal data in systems used exclusively for statistical reporting and research should be protected by statute from compulsory disclosure in identifiable form.[76] An organization should make no transfer of individually identifiable data to another organization without the consent of the individual.[77] Any organization maintaining an automated personal data system used exclusively for statistical research and reporting should give public notice of that fact.[78] This requirement would give some assurance that there would be no secret automated data systems and that the uses of these systems by organizations to help influence social policy or behavior would be accessible to independent expert scrutiny.[79]

C. *Computers for Third-Party Medical Payers*

The use of computers for third-party payment is currently the most prevalent use of computers. Third-party payers include government agencies, non-profit entities such as Blue Cross-Blue Shield, other pre-paid plans such as HIP in New York City, and health and accident insurance plans.[80] Great quantities of medical data are processed, including personally identifiable information. One trade association is reputed to maintain a computerized center which stores information on millions of persons throughout the country. Members may inspect information which is estimated to be held on ninety-nine percent of all persons with life insurance issued in the United States.[81] Many companies in the industry have long shared underwriting data. If an individual previously sought insurance from a participating company, his file may contain large quantities of data, including the condition diagnosed, its overall effect, its current status, the treatment plan, and the doctor, hospital, or clinic involved.[82] The source of this information could very well be the applicant himself. Besides the applicant's possible motive to distort, or difficulties in recalling precise medical information, the insurance salesman is also motivated to dis-

---

76. *Id.* at 86-87. "There are few statutes that protect personal data in statistical reporting and research files from unintended administrative or investigative uses. The Census Act, the Public Health Service Act, and the Social Security Act are notable exceptions." *Id.* at 92-93.

77. *Id.* at 97.

78. *Id.* at 99.

79. *Id.* at 100.

80. Boyer, *supra* note 51, at 51-52.

81. *Hearing on Commercial Health and Accident Insurance Industry Before the Subcomm. on Antitrust and Monopoly of the Senate Comm. on the Judiciary*, 92d Cong., 2d Sess., pt. 1 at 38 (1972) (hereinafter cited as *Hearings on Commercial Health Insurance*).

82. Boyer, *supra* note 51, at 54.

tort the facts. If his client's application for insurance is turned down he does not get his commission. Further, this information is often obtained by an independent investigative reporting agency.[83]

One agency is reputed to be responsible for approximately fifteen million annual investigative reports, of which seventy percent are insurance reports.[84] The number of investigations completed each day, coupled with the use of hearsay information, have contributed to distorted, sloppy, and inaccurate profiles of individuals. The flavor of these operations can be gained from the following description of a field investigator inquiring about his suspicion that his subject is having an extramarital affair:

> You go to a neighbor and establish rapport . . . . Then you ask, What's your opinion of X's home life; how do you think of him as a family man? This will usually elicit some hint . . . . Then you start digging. You press them as far as they go, and if they become recalcitrant, you go somewhere else.[85]

In a complaint against an investigative reporting agency, the Federal Trade Commission alleged the retention of this insurance data in their files for subsequent use or sale.[86] Some insurance companies and employers are lucrative markets for this information. Organizations which use these services may know more about an individual's medical condition than the individual, since medical ethics do not allow a patient to see his own records.

Do credit companies have the "right" to see or give the information they collect about people to other agencies?[87] Theoretically and morally, a strong argument could be made for an answer in the negative. Legally, however, this practice is difficult to prevent. The legal system has generally not treated personal information as the property of the subject and has, therefore, allowed a true market system for such information to develop. Until such information is deemed a property interest of the data subject, and legislative restrictions are developed, this "black marketeering" will continue.[88] Current laws

---

83. Miller, *supra* note 25, at 69.

84. *Id.* at 69-70 (footnote omitted).

85. *Id.*

86. *Hearings on Commercial Health Insurance*, *supra* note 81, at 118.

87. It is beyond the scope of this paper to explore in depth the underwriting claims processing industry.

88. *See, e.g.*, Goldstein, *Information Systems and the Role of the Law: Some Prospects*, Book Review, 25 STAN. L. REV. 449, 473-75 (1973). It has been expressed that there is no theoretical reason why an individual's privacy right could not be valued by a market system in which the data subjects employ essentially licensed data users to have access to

are inadequate to protect individuals against this prevalent conduct throughout the country engaged in by some of the largest companies.[89] Unfortunately, medical records may be useful for a variety of purposes other than diagnosis and treatment. For instance, would a bank want to make a loan to a person with a terminal disease?

Trade associations, however, are insignificant compared to Medicare and the Social Security Administration (SSA).[90] Although a myriad of problems exist which threaten the individual's privacy, it is ironic that the more the data processing organization attempts to be open and responsive to its clientele, rather than bureaucratic and remote, the greater the possibility of leakage. An SSA official expressed the dilemma as follows:

> We are kind of in the middle between the need to efficiently serve the people, which is our basic function, and the need to protect the privacy and confidentiality of our records.
>
> In taking 4, 5, or 6 million claims a year and processing 18 million postentitlement earnings and posting 343 million earnings items, . . . we must set up systems and operations so that the district office personnel can get the information readily and efficiently.
>
> Now if we put too many restrictions on obtaining it, then we would have to get too much [identification or authorization] from people [who are requesting information about this entitlement status], or so much information that it would be difficult to respond to our mission.[91]

Further, the more comprehensive and accurate the data base, the greater the temptation will be to use it for non-medical purposes, including commercial gain. It is interesting to note that the SSA has discovered that the greatest threat is not from illegal intruders, but rather from perfectly legitimate organizations and interests seeking to obtain access through political or other legal means. For example, attorneys seek information helpful to their clients and frequently attempt to collect information by subpoena. Others who seek information include missing persons bureaus, skip traces organizations,[92]

---

personal information, analogous to a copyright proprietor licensing various uses of a book or song. *Id.* at 474

89. Linowes, *supra* note 32, at 1182.

90. Boyer, *supra* note 51, at 61-62.

91. *Id.* at 70. (quoting *Hearings on Federal Information Systems* (testimony of Richard D. Shepard, Director, Division of Systems Coordination & Planning, Office of Administration, Social Security Administration) at 334).

92. A skip trace organization, like a missing persons bureau, gathers information

business firms seeking information about competitors, as well as political and commercial organizations requesting lists of names.[93]

In order to solve many of the problems raised, a large scale structural change in health care programs is necessary. There is a clear trend in third-party payment toward the steady expansion of benefits and beneficiaries.[94] As publicly funded health care becomes more expansive, everyone becomes a welfare recipient to some degree and thus joins a group whose privacy has traditionally been sacrificed to administrative convenience and pressures for public accountability. When health benefits are narrowly limited or defined to particular groups such as income, nature of illness, or type of provider, it becomes necessary to gather detailed information to be certain that the eligibility requirements are met. Therefore, simplifying eligibility standards could make it possible to reduce the amount of personal data needed. Additionally, replacing separate and parallel programs with a unified government program could reduce the need to use computers as surveillance devices to track down individuals who are not really eligible for certain benefits.[95] Publicly funded health care programs have many political and practical considerations, however, making it unlikely that privacy will be of paramount importance.[96]

The private sector is controlled only by limited privacy protections. It is unlikely that they will voluntarily police themselves and set standards that will protect the privacy of individuals. Privacy in the private sector will evolve further only if there is general public pressure. One insurance executive has characterized an insurance applicant's authorization form as a "search warrant without due process."[97] It authorizes the release of all information, it has no expiration date, and it indicates that a copy is as valid as the original.[98] Efforts to protect *medical privacy*, therefore, have tended to focus on legal and administrative controls, rather than on theoretical or practical justifications for protecting the data in the first place.[99]

Traditional legal controls have not met the challenge, nor an-

---

about persons who have either disappeared or have moved without leaving a new address. *See* Boyer, *supra* note 51, at 71, n.129.

93. Boyer, *supra* note 51, at 71, n.129.

94. *Id.*

95. *Id.* at 73-74.

96. *Id.*

97. Linowes, *supra* note 31, at 1182.

98. *Id.*

99. Boyer, *supra* note 51, at 76. Whether or not we want to prevent collection of information in the first instance or whether there should be justification of its use once it has been collected remains an issue in all areas of information collection and use.

swered the need. Privilege statutes do not solve the problem.[100] They are designed to govern disclosures in an official forum. Further, signing a consent form is no longer a knowing and voluntary waiver of one's rights, but can be analogized in medical situations to contracts of adhesion where there is really no choice. The waiving of an injured person's right to sue is the most significant weakness in today's common law privacy action. The principal difficulty with the consent defense is the insensitivity to the individual's plight when he is faced with the prospect of losing all medical benefits.

In assessing whether an individual's consent is truly voluntary, all of the surrounding circumstances should be considered.[101] Too often the intrusive offender escapes the responsibility and the loss of privacy is blamed on the victim.[102] The focus on genuine informed consent to medical procedures and disclosure of medical information might provide some real guidance in this area. Legislative recognition in support of prohibiting certain requests, and requiring adequate disclosure of the risks, is long overdue.

Traditional privacy and privilege doctrines are creatures of diverse state statutory or common law provisions. A major obstacle to the recognition of the privacy right is the fact that without uniform national standards, privacy is determined on a state by state basis. It is extremely difficult to apply these privacy rights to a system that is most often part of multi-state or multi-national communication networks. Perhaps this recognition of privacy rights and privileges must be joined with greater legislative controls. Common law causes of action for the invasion of privacy were not formulated with the objective of regulating the disclosure of medical information. The prevailing systems and statutes have not contributed to confidentiality, unless

---

100. *Id.*

101. *Id.*

102. *See, e.g.*, Miller, *supra* note 25, at 86 (quoting *Hearings on Commercial Credit Bureaus Before a Subcommittee of the House Committee on Gov't Operations*, 90th Cong., 2d Sess. (1968)).

> A blatant example of an attempt to hide behind the consent shield to immunize practices is one national credit bureau's reaction when it became alarmed by a congressional investigation and the prospect of subsequent regulation. It began to include the following clause in its credit application form:
>
> I hereby authorize the person to whom this application is made, or any credit bureau or any other investigative agency employed by such person, to investigate the references herein listed, or statements, or other information, oral or written, obtained from me or any other person pertaining to my credit and financial responsibility. . . . I hereby release any claims, damages and suits whatsoever which may at any time be asserted by me by reason of such investigation.

Id.

"confidentiality" includes protecting the patient from securing information about himself. The advent of computers, however, has stimulated a long overdue concern for privacy that might prove beneficial if it can be sustained. This obvious threat to privacy has triggered a needed awareness. The real challenge is to devise a method for balancing the competing interests of privacy against other significant social benefits.

III. ATTEMPTS AT PARITY: THE ESTABLISHED LEGAL CONTROLS

A. *Constitutional Recognition*

1. Origins

Privacy is not specifically mentioned in the United States Constitution. The Constitution has, however, provided the source for the right to privacy. The Supreme Court has recognized that "a right of personal privacy, or a guarantee of certain areas or zones of privacy" does exist under the Constitution.[103] The Court has found the roots of that right in the First Amendment,[104] Third Amendment,[105] Fourth Amendment,[106] Fifth Amendment,[107] Ninth Amendment,[108] the due process clause of the Fourteenth Amendment,[109] and in the penumbras of the Bill of Rights.[110] This American right to privacy is an individual constitutional right, but one which is not absolute. Courts have refused to recognize an unlimited right to privacy in the past. States have compelled the sterilization of certain individuals,[111] and vaccinations in circumstances where there has been a compelling state interest.[112]

---

103. Roe v. Wade, 410 U.S. 113, 152 (1972).

104. *E.g.*, Stanley v. Georgia, 394 U.S. 557, 563 (1969)(holding that the First Amendment guarantees freedom of speech and assembly).

105. The Third Amendment prohibits the lodging of soldiers in private homes. U.S. CONST. amend. III.

106. The Fourth Amendment protects citizens from being searched arbitrarily by the government. U.S. CONST. amend. IV.

107. Courts interpret a right to privacy in the Fifth Amendment which protects against self-incrimination. U.S. CONST. amend. V.

108. Griswold v. Connecticut, 381 U.S. 479 (1965). The Ninth Amendment gives the people all rights not specifically delegated to the States and Federal government. *Id.* at 492 (Goldberg, J. concurring).

109. The Fourteenth Amendment guarantees each citizen equal protection of the laws. U.S. CONST. amend. XIV.

110. *See, e.g.*, Roe v. Wade, 410 U.S. 113, 152 (1973).

111. Buck v. Bell, 274 U.S. 200, 207 (1927). *But see* Skinner v. Oklahoma, 316 U.S. 535 (1942). The Supreme court has increasingly recognized an individual's rights with regard to procreation. *Id.*

112. Jacobson v. Massachusetts, 197 U.S. 11, 38-39 (1905).

2. Developments

The Supreme Court ruled in *NAACP v. Alabama*[113] that there is a constitutional right to privacy in one's associations.[114] In *Tulley v. California*[115] the Court affirmed the necessity of anonymous political activity for the proper functioning of free society.[116] In *Griswold v. Connecticut*[117] the Supreme Court invalidated a Connecticut statute which made it a crime to use contraceptives. Justice Douglas reasoned that there were private rights surrounding various amendments to the Constitution and specifically mentioned the First Amendment zone of privacy with regard to private personal functions.[118]

Four years later, the Court in *Stanley v. Georgia*[119] struck down Georgia's law which made it illegal to possess pornography in one's home. The Court held that the government cannot pry into one's thoughts, feelings, and mind.[120] In *Wisconsin v. Constantineau*[121] the Supreme Court invalidated a Wisconsin statute which permitted a police chief to post a list of persons whom he thought were alcoholics. The purpose of the list was to prohibit others from contributing to the addiction of those listed by not providing them with alcoholic beverages.[122] The Court, however, recognized the Constitutional implications of an invasion of personal privacy that could permanently label an individual.[123]

A Texas statute banning abortion was invalidated in *Roe v. Wade*.[124] The Court held that there was a violation of the right to privacy as "founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action."[125] The importance of procreative autonomy as an element of individual liberty was reaffirmed in *Eisenstadt v. Baird*.[126] There now exists a private realm of family life which the state cannot enter. There is a constitutionally

113. 357 U.S. 449 (1958).
114. *Id.*
115. 362 U.S. 60 (1960).
116. *Id.* at 64-65.
117. 381 U.S. 479 (1965) (holding that the zone of privacy is created by several fundamental constitutional guarantees as specific guarantees in the Bill of Rights).
118. *Id.* at 485.
119. 394 U.S. 557 (1969).
120. *Id.* at 565.
121. 400 U.S. 433 (1971).
122. *Id.* at 435, n.2.
123. *Id.* at 437.
124. 410 U.S. 113 (1973).
125. *Id.* at 153.
126. 405 U.S. 438 (1972). The *Eisenstadt* Court recognized that procreative autonomy includes both the right to remain fertile and the right to avoid contraception. The

protected right to privacy, which means that an individual may make procreative decisions without governmental interference.

The Supreme Court's focus with respect to privacy has been on personal autonomy and freedom from governmental interference. The Court's decisions recognizing a constitutional privacy right in these areas raised the possibility that a general right to privacy for matters relating to medical treatment might emerge and restrict the government's power to gather medical records.[127] This possibility, however, remains unrealized.

In *Schulman v. New York City Health and Hospitals Corp.*[128] a city ordinance was upheld requiring that names of abortion patients be reported on a "termination of pregnancy" certificate which is then filed in a central registry.[129] The court held that the constitutional privacy claim must fail because there was a compelling state interest to provide statistical information about the effect of abortions and to provide counseling on family planning.[130]

Although the Supreme Court's recent decisions have not dealt specifically with the collection of medical data, in *California Bankers Ass'n v. Schultz*[131] the Court held that there was no right to privacy protection in bank records kept by a bank in accordance with federal regulations.[132] Additionally, the Court held that the Fourth Amendment challenges to the reporting requirements failed because the statutory purposes were reasonable.[133] Moreover, the bank could not challenge the requirements on the ground of self-incrimination,[134] and the depositer plaintiffs lacked standing to challenge the domestic re-

---

Court pointed out that the intimacy and gravity of contraceptive decisions are not lessened by the absence of marriage. *Id.* at 453.

See also Carey v. Population Services Int'l., 431 U.S. 678 (1977). The Carey Court reaffirmed both the right of all persons to make contraceptive decisions, and the fundamental right of autonomy in the decision whether or not to beget or bear children. *Id.* at 684-85.

127. Boyer, *supra* note 51, at 89. *See e.g.*, Doe v. Bolton, 410 U.S. 179, 219 (1973) (Douglas, J., concurring)("the right of privacy has no more conspicuous place than in the physician-patient relationship").

128. 44 A.D. 2d 482, 355 N.Y.S.2d 781 (1974).

129. *Id.* at 483, 355 N.Y.S.2d at 782.

130. *Id.* at 486, 355 N.Y.S.2d at 485. *See also* Whelen v. Roe, 429 U.S. 589 (1977) (upholding a statute requiring physicians to report certain prescriptions given for barbiturates).

131. 416 U.S. 21 (1974).

132. *Id.* at 66-67.

133. *Id.* at 67.

134. *Id.* at 75. The challenge, however, was premature. The court left the issue of whether the bank could claim the privilege for resolution when the challenge is properly before the court. *Id.*

porting regulations.[135] It appears that the Court is willing to defer the regulation of data collection to other branches of government. Thus, the Court has not expanded constitutional privacy broadly into informational policy areas.[136]

B. *Common Law*

1. Background

The concept of privacy was not recognized at English common law. Samuel D. Warren and Louis D. Brandeis first introduced the idea of a legal right to privacy in a law review article.[137] They declared privacy to be "a part of the person"[138] and asserted that there was a right to be free from publicity when one had not voluntarily placed himself under public scrutiny. They analogized the privacy right to the right of an individual to be free from unwarranted publication of his name or personal information.[139] Despite the authors' persuasiveness, however, their thesis was opinion, not law. It remained for the courts to give it their imprimatur.[140] The first major test came in the case of *Roberson v. Rochester Folding Box Co.*,[141] in which a milling company used a woman's picture without her consent to promote the sale of its flour. The court rejected her claim for relief based on her humiliation. The court held relief would have to come from the legislature.[142] The New York Legislature did respond and other states followed.[143] Courts in almost every state eventually began to recognize a person's right to seek a remedy for an invasion of privacy.[144]

2. Privacy Torts

Professor William L. Prosser defined four kinds of privacy torts

---

135. *Id.*

136. *See, e.g.*, Paul v. Davis, 424 U.S. 693, 712-13 (1976). In this case the plaintiff's picture had been circulated to town merchants as an active shoplifter. He had been charged, but never prosecuted for the offense. The plaintiff sued the Chief of Police for violating his constitutional right of privacy. The Court held that this case was not within the "zones" of recognized rights. *Id.* at 713.

137. Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

138. *Id.*

139. *Id.*

140. Miller, *supra* note 25, at 171.

141. 171 N.Y. 538, 64 N.E. 442 (1902).

142. *Id.* at 544, 64 N.E. at 443.

143. *See infra* notes 253-255 and accompanying text.

144. States are not consistent with regard to the dimensions of a person's right to privacy.

which were recognized at common law:[145] (1) Intrusion upon the plaintiff's physical solitude or seclusion; (2) public disclosure of private facts; (3) false light in the public eye; and (4) appropriation of one's name or likeness for the commercial benefit of another.

The tort of intrusion extends to eavesdropping[146] and the use of microphones.[147] Professor Arthur Miller concluded that although the intrusion concept may be a useful approach for remedying wiretapping, electronic eavesdropping, or physical or sensory surveillance, it does not afford much protection against misuse of computerized information.[148] He reasoned that the privacy tort is designed to deter direct physical invasion which is not the case with computerized information.[149] Additionally, the tort deals with the nature of the conduct that constitutes the privacy violation rather than what is done with the fruits of the invasion. In the context of computerized information, it is what is done with the data that presents the greatest threat to privacy.[150]

The public disclosure of private facts has found a cause of action in the publicity of highly private information. Even if the information were true and there would be no action for defamation, a cause of action may still exist.[151] This tort may be most applicable to computer cases and the abuses that are likely to arise in modern medical record systems. There are problems, however, as the private facts must be disclosed to the public at large. "The few reported cases involving medical information seem to arise out of sensationalized reports of freakish maladies"[152] or case history studies in which the researcher has failed to conceal the subject's identity.[153] An unauthorized user of an individual's computerized file can use the misappropriated data to damage its subject *without* further disseminating its contents. Additionally, the disclosed information must be information normally considered to be private. This could always be the subject of considerable dispute. Professor Miller contends that if sensitive material is commingled with less sensitive material in a computer, the entire mass of

145. W. PROSSER, LAW OF TORTS, 804-814 (4th ed. 1971).

146. *See, e.g.*, Fowler v. Southern Bell Tel. & Tel. Co., 343 F.2d 150 (5th Cir. 1965).

147. *See, e.g.*, Elson v. Bowen, 436 P.2d 12 (1967).

148. Miller, *supra* note 25, at 171.

149. *Id.*

150. *Id.* at 174.

151. PROSSER, *supra* note 145, at 809.

152. Boyer, *supra* note 51, at 79.

153. *See, e.g.*, Doe v. Roe, 33 N.Y.2d 902, 307 N.E.2d 823 (1973). A psychotherapist published a book on intimate relations about a patient and her family. Plaintiff claimed that she and her family were easily identifiable. *Id.*

data may be given less protection because it may be treated as low level sensitivity.[154] The final requirement is that the disclosure must be offensive to a person with ordinary sensibilities.[155] Miller suggests, however, that we might become accustomed to the revelation of the intimate details of a person's life just as we have become accustomed to offensive television commercials.[156]

False light is similar to if not indistinguishable from defamation. The common law of defamation involves the publication of false information that injures reputation: "A communication is defamatory if it tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him."[157] If a publication harms the reputation of another by subjecting him to hatred or shame, a cause of action for defamation will lie. Since the statement must be false, there is no conflict with the First Amendment which arguably protects only the truth.[158] The Supreme Court expanded this requirement in the landmark case of *New York Times Co. v. Sullivan*.[159] The Court held there could be no liability for defamatory falsehoods unless it was known that the statement was false, or made with reckless disregard to the truth.[160] The holding applied to public officials and was subsequently extended to public figures.[161] The Court, however, refused to extend this requirement to non-public figures and ordinary citizens.[162] The Court, in *New York Times Co. v. Sullivan*, addresses only defamation. Privacy, however, is addressed when publication is an element of the tort.

The false light principle should be expanded to permit law suits by those who are injured by information which is disclosed and is misleading. Additionally, the courts should de-emphasize the requirement of disclosure at large "if the theory is to be responsive to the way in which computerized information will be used in a dossier

---

154. Miller, *supra* note 25 at 174.

155. The ordinary sensibilities standard parallels the reasonable person standard in tort law. For more complete treatment of the reasonable person standard. *See* PROSSER, *supra* note 145, at 149-166.

156. Miller, *supra* note 25, at 177-78.

157. RESTATEMENT OF TORTS § 559 (1938).

158. Trubow, *Fighting off the New Technology*, 10 Human Rts. 27, 28 (1982).

159. 376 U.S. 254 (1964).

160. *Id.* at 280.

161. Curtis Publishing Co. v. Butts, 388 U.S. 130 (1967).

162. Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974). *See* Cantrell v. Forest City Publishing Co., 419 U.S. 245 (1974) (leaving open the question in a false light privacy invasion case whether there should be a lesser standard than that applied in *Sullivan*). *See also* Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 494-95 (1975) (holding that "the interests in privacy fade when the information involved already appears on the public record.").

society."[163]

Should the criterion for triggering a privacy claim be tangible injury, or simply outrage and emotional distress from wrongfully disclosed information? Should privacy be protected as Warren and Brandeis first suggested, in the notion of "inviolate personality," or merely in a property context after a pecuniary loss?[164] Further, should one be compensated for lost opportunity due to the wrongful disclosure of information? Can Senator Eagelton ever be compensated for the lost opportunity of being elected vice-president and perhaps even succeeding to the White House?

3. Privacy as a Property Interest

It may be easier to formulate privacy guidelines in a property context. It has been suggested that personal information be recognized as a property interest under traditional property law. A cause of action would, therefore, be available to a victim for information abuse because as "owner" of the information there would be an abuse of his interest.[165]

Further, who is entitled to privacy, individuals only, or corporations and government? Additionally, should an information policy govern information practices of individuals? What about the computer enthusiast with a home computer? Even national data banks are accessible by personal computers. At common law, the concept of privacy was modeled on mass dissemination and thus extremely restrictive. Typically the common law of informational privacy was designed to compensate a victim after intimate personal information was divulged about him in one of the mass media.[166] To establish a claim, an individual must prove a disclosure of personal facts to the public.

Personal privacy as developed by the courts has been in reaction to the media of mass communication. Usually the individual will see it or it will be brought to his attention and he will respond to it with a law suit. Computers present a more complicated situation. You are not dealing with a mass dissemination; something you can see and hear and respond to, and if you are aggrieved, take the publisher to court. You are dealing with records stored somewhere in electronic

163. Miller, *supra* note 25, at 184-85.

164. Trubow, *supra* note 158, at 52.

165. Miller, *Symposium: Computers, Data Banks and Individual Privacy*, 53 MINN.L.REV. 212 (1968).

166. *Hearings, Federal Data Banks, supra* note 4, at 17.

form in some federal or state agency or some corporation or university, of which the individual probably has no knowledge.

> . . . [T]he person most concerned with the information, the person who will be affected by others seeing and acting on it, often has the least access to it. The law of privacy as we know it today simply has not developed or reacted to this problem.[167]

C. *Legislative Recognition*

Neither the common law privacy right, nor the existing statutory situation is adequate to handle the need to strike the appropriate balance between the individual's need for privacy and society's need for information. Nevertheless, it is Congress and the states to which we must look for the protection of informational privacy. Since privacy is not specifically mentioned in the Constitution and because of the specific protection given speech and press in the First Amendment, the answer appears to rest with the legislature. Additionally, the establishment of agencies might be a possible solution and only Congress is capable of developing broad guidelines for these agencies. The judiciary is not capable of this task.[168]

The Fair Credit Reporting Act of 1970 (FCRA) was the first legislative recognition of the right of the individual citizen to have access to his or her informational profile.[169] It was also the first federal legislation enacted to regulate personal information maintained by the private sector. The Act requires that credit investigation and reporting agencies make their records available to the data subject.[170] Additionally, the agencies must provide procedures to correct information and to respect the confidentiality and proper utilization of the information. Individuals may challenge the fairness, accuracy, and timeliness of the information.[171] The individual, not the business entity, is protected under the FCRA. Moreover, it is interesting to note that consumer credit reports are deemed commercial speech, which is outside the protection of the First Amendment.[172] The FCRA has been the only

---

167. *Id.*

168. Not everyone is convinced that legislative controls over personal data systems are necessary. Robert H. Long, Director of ACT, Bank Administration Institute, has stated: "The way to protect privacy and confidentiality is to improve the procedures of redress, not to attempt to control every personal data file at a government level." PRIVACY AND SECURITY IN COMPUTER SYSTEMS, *supra* note 11, at VIII.

169. 15 U.S.C. §§ 1681-1681t (1976 & Supp. 1980).

170. *Id.* § 1681g.

171. *Id.* § 1681i.

172. *Id.*

significant attempt at the federal level to impose information privacy rights on the private sector. The Act requires that an individual be notified when an adverse action (such as denial of credit) is taken on the basis of a report from an agency.[173]

The Act, however, has major inadequacies. The list of people to whom disclosure is permitted is both too vague and too broad. It includes anyone with a "legitimate business need" for information.[174] Moreover, enforcement authority rests with the Federal Trade Commission which has been lax.[175] Further, "few consumers have the funds necessary to engage in expensive litigation when the Federal Trade Commission declines to act."[176]

The most comprehensive regulatory scheme is contained in the Privacy Act of 1974.[177] The Act applies to information systems which are operated by the federal government. The Act does not deal with data systems operated by private organizations or state and local governments.[178] It attempts to promote governmental respect for the privacy of citizens by requiring agencies to observe certain rules in the computerization, use, and disclosure of information.[179]

The goals of the Act were set forth in the HEW Report: (1) There should be no secret data record-keeping systems; (2) an individual should be able to find out what information is on record about him; (3) there must be a way for an individual to prevent information collected about him for one purpose from being used for another purpose; and (4) an individual should be able to correct inaccurate information.[180]

---

173. *Id.* § 1681m.

174. 12 U.S.C. § 1681b(3)(E).

175. Washburn, *Electronic Journalism, Computers and Privacy*, 3 COMPUTER/L. J. 189, 195 (1982) (quoting Halls, *Raiding the Databanks: A Developing Problem for Technologists and Lawyers*, 5 J. CONTEMP. L. 256 (1979)).

176. *Id.*

177. 5 U.S.C. § 552a (1976 & Supp. 1980).

178. *Id.*

179. *Id.*

180. HEW REPORT, *supra* note 36, at XX. Specifically the report recommended the enactment of a Federal Code of Fair Information Practice resting on five basic principles that would be given legal effect as "safeguard requirements" for automated personal data systems:

> There must be no personal data record-keeping systems whose very existence is secret.
>
> There must be a way for an individual to find out what information about him is in a record and how it is used.
>
> There must be a way for an individual to prevent information about him that

The Act provides for access by data subjects.[181] Additionally, it requires procedures for the correction of challenged information.[182] Moreover, no disclosure of personal information may be made without written consent.[183] The Act imposes limitations on data collection about individuals to information which is relevant and necessary to accomplish a legitimate agency purpose. The agency must maintain records with accuracy, relevance, timeliness, and completeness to assure fairness to the individual.[184] The Act established four actions for civil remedies. An individual may bring an action if the agency fails to comply with the Act's requirements: by failing to amend an individual's record in accordance with his request;[185] by failing to maintain an individual's record in the above prescribed manner;[186] or by not complying with the Act in such a way as to cause an adverse effect on the individual.[187] An individual may bring an action to compel production of his records and the court may enjoin the agency from withholding such records.[188] In addition, the court may order an agency to amend an individual's records in accordance with his request.[189] An individual may recover actual damages[190] and reasonable attorney fees and other litigation costs[191] in appropriate situations. Jurisdiction lies with district courts of the United States.[192]

---

was obtained for one purpose from being used or made available for their purposes without his consent.

There must be a way for an individual to correct or amend a record of identifiable information about him.

Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of data.

Id.

181. 5 U.S.C. § 552 a(d) (1982).

182. *Id.*

183. 5 U.S.C. § 552 a(b)(1974). Some of the exceptions are important. They include disclosure to the National Archives of the United States, *Id.* § 552 a(b)(6); Bureau of Census, *Id.* § 552 a(b)(4); to another agency or instrumentality of the government for a civil or criminal law enforcement activity, *Id.* § 552 (b)(7); to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual, *Id.* § 552 a(b)(8); to either House of Congress, *Id.* § 552 a(b)(9); pursuant to the order of a court of competent jurisdiction. *Id.* § 552 a(b)(11).

184. *Id.*

185. *Id.* § 552 a(g)(1)(A)(B).

186. *Id.* § 552 a(g)(1)(C).

187. *Id.* § 552 a(g)(1)(D).

188. *Id.* § 552 a(g)(3)(A).

189. *Id.* § 552 a(g)(2)(A).

190. *Id.* § 552 a(g)(4)(A). The act provides for minimum damages of $1,000 in cases in which the agency violates the act wilfully or intentionally. *Id.*

191. *Id.* §§ 552 a(g)(2)(B); 552 a(g)(4)(A); 552 a(g)(4)(B).

192. *Id.* § 552 a(g)(1)(D).

With regard to medical records, the extent to which this approach of notice and opportunity to object can be effective in eliminating improper agency practices depends on the participation of consumer and provider groups such as public interest groups involved in health care issues, medical societies concerned about government intrusions on the doctor-patient relationship, or other related associations which are able to provide guidance.[193]

The Act has been criticized because it is confined to federal systems. Many commentators feel that the consumer's right of privacy is "far more vulnerable to computerized invasion by the private sector than by government agencies."[194]

The Act did create a Privacy Protection Study Commission to investigate the private sector and make recommendations.[195] The Privacy Protection Commission made one hundred sixty-two specific recommendations.[196] There were three major public policy objectives:. to minimize intrusiveness; to maximize fairness; and to create a legitimate and enforceable expectation of confidentiality when this expectation is warranted. In order to accomplish these objectives, the Commission recommended that certain principles be adhered to: only information relevant to the particular matter at hand should be collected; information should not be transferred to third parties without the subject's approval; the individual should be informed as to what sources will be contacted in order to gather information and how it will subsequently be used; an individual should have the right to see any file about him and be able to correct inaccurate information; secret files should be outlawed; proper authorization of government officials should be required before they are permitted access to files; and organizations should only employ service and support firms whose privacy standards are substantially similar to the organization being served.[197]

The Commission urged that individuals be afforded a right of action against offenders of these principles. Court costs, actual damages, and general damages of $1,000 to $10,000 should be recoverable. The substance of the recommendations was to chip away at the constructive "property right" which organizations asserted with respect to the

193. *Id.*

194. Washburn, *supra* note 175, at 193.

195. This Commission was established by P.L. 93-579, § 5 88 stat. 1905 (1984) codified in 5 U.S.C. § 522 (a)(1977), and ceased to exist on Sept. 30, 1977 by the terms of the enactment as amended by P.L. 95-38, 91 stat. 1979 (1977).

196. PRIVACY COMMISSION REPORT, *supra* note 3, at 3-4.

197. *Id.*

personal information maintained in their files.[198]

The Act has many weaknesses. Litigants may be deterred because of the low visibility of many information misuses, being unable to identify a direct causal relationship with a denial of a benefit to a violation of the statute. Further, disclosure may be immunized under an exception. The difficulty of proving the requisite intent for actual damages may render litigation worthless. The ultimate burden falls on the consumer. Despite its limitations, the Privacy Act of 1974 was a significant, although tentative step towards evolution of a comprehensive system of legal safeguards for information about individuals.[199]

The Family Educational Rights and Privacy Act of 1974[200] requires schools and colleges which receive federal funds to grant students or their parents access to student records and restricts disclosure of such information to third parties.[201]

The Tax Reform Act of 1976[202] provides for the confidentiality of individual tax returns and limits disclosure to third parties. The Right to Financial Privacy Act of 1978[203] provides bank customers with privacy regarding their bank's records by giving individuals notice and a chance to challenge requests by federal agents for the records.[204]

The Privacy Protection Act of 1980[205] gives protection against the search and seizure of materials in the possession of the media such as a newspaper's records or files by law enforcement authorities including federal, state, and local agencies.[206] Only if the custodian of the materials is suspected of criminal activity or in order to prevent death or serious bodily harm will these safeguards be waived.[207] The

198. *Id.*

199. Boyer, *supra* note 51, at 95.

200. 20 U.S.C. § 1232g (1976) *amended by* 20 U.S.C. § 1232g(5) (Supp. III 1979).

201. The Family Education Rights and Privacy Act of 1974 is popularly referred to as the Buckley Amendment.

202. 26 U.S.C. § 1 (1976).

203. 12 U.S.C. §§ 3401-3422 (Supp. IV 1980).

204. In 1976 the United States Supreme Court in United States v. Miller, 425 U.S. 435 (1976) held that an individual had no expectation of privacy with regard to his bank records, as they were the property of the bank. *Id.* The Right to Financial Privacy Act of 1978 was in direct response to *Miller* and thus overruled the decision. In addition Congress inserted the Tax Reform Act of 1976, Pub. L. No. 94-455, 90 Stat. 1520 (1976), which states that the government must give notice to a taxpayer when it serves a summons from the Internal Revenue Service.

205. 42 U.S.C. § 2000aa (Supp. IV 1980).

206. The Act is in contradiction to Zurcher v. Stanford Daily, 436 U.S. 547 (1978), which upheld the right of the police to search a student newsroom, and consequently caused much concern amongst the press and ordinary citizens as well.

207. 42 U.S.C. § 2000 aa(b) (1982). The exceptions to surprise searches are: (1) if the reporter or author can reasonably be suspected of having committed the crime being

Attorney General is directed to issue procedural guidelines by the law with respect to obtaining materials in the possession of other innocent persons.[208] Subsequently, the Department of Justice restricted the use of search warrants where subpoenas will suffice when seeking documents, tape recordings, or similar material from journalists, lawyers, doctors, and clergymen who are not suspected of any crime.[209]

The Electronic Fund Transfer Act of 1980 requires banking institutions using electronic fund transfers to notify their customers about any third-party access to customer accounts.[210]

The Freedom of Information Act of 1966[211] represented significant legislation in delineating the individual's rights to privacy. Present government information policy is primarily regulated by the Freedom of Information Act (FOIA) and the Privacy Act of 1974. The FOIA gives every person the right to review government records. Federal agencies have authority to withhold personal data which would constitute a clearly unwarranted invasion of privacy.[212] The agency, however, not the individual, is given discretion to decide which disclosures meet this criterion.[213] The Act has been criticized as "an instrument for disclosing information rather than for balancing the conflicting interests that surround the public disclosure and use of personal records."[214] In fact, the 1974 Privacy Act's Conditions of Disclosure Section reflects the Congressional response to the potential for abuse of disclosure regarding personal information.[215]

The individual's right to know prevails in the 1966 Act, and federal records are available for public inspection and copying. This has actually made the Act and privacy conflict. The Act opens records to everyone, which is in direct conflict to the data subject's desire to keep his records private and confidential. Further, the Act has unfortunately been used for improper purposes and benefits the wrong people. Many people have used the Act successfully to obtain information

---

investigated; (2) if serious injury or death will result if the materials are not immediately seized; (3) if the materials would be destroyed or altered if advance notice of a subpoena were given; and (4) if an individual has failed to turn over materials that have been legally subpoenaed. *Id.* § 2000aa(b).

208. *Id.* § 2000aa-11.

209. 46 Fed. Reg. 1302, 1303, 1304 (1981).

210. 15 U.S.C. 1693 (1982 Supp.)

211. 5 U.S.C. § 552 (1976).

212. HEW REPORT, *supra* note 36, at 35. *See* 5 U.S.C. § 552 a(b) (1982).

213. 5 U.S.C. § 552a b(1)-(9) (1982).

214. HEW REPORT, *supra* note 36, at 35.

215. Comment, *Federal Legislative Proposals for the Protection of Privacy*, 8 FORD. URB. L. J. 773,787 (1979).

about business competitors or adversaries in litigation.[216] Professor Arthur Miller has stated that the "Act probably does more to end privacy in the United States, ostensibly in the pursuit of the public's right to know than any other enactment in the last 50 or 60 years."[217] It is a difficult task for federal agencies and courts to balance the public's right to know against an individual's right to privacy.[218] Further, the terms of the Act are inadequate for dealing with computerized record-keeping. It deals with only two aspects of record-keeping practice-data collection and data dissemination.[219]

The Federal Reports Act of 1976[220] requires that federal agencies get approval from the Office of Management and Budget before collecting "information upon identical items from ten or more persons."[221] The purpose of the Act was to maximize the usefulness of the information collected, rather than to further personal privacy. The Act makes no mention of personal privacy "nor recognizes any rights for individuals with respect to the personal-data record-keeping practices of the federal government."[222]

IV. COMPUTER SECURITY

Many believe that safeguarding the privacy of individuals is a matter properly reserved for the legislature, but that solutions for protecting confidential data in automated systems are to be found in technological safeguards.[223]

Infringements on individual privacy although extensive should not be accepted as an inevitable outgrowth of technological advance-

---

216. Freedman, *The Right of Privacy in the Age of Computer Data and Processing*, 13 TEX. TECH. L. REV. 1361, 1380 (1982).

> Congress did not intend to permit litigants to use the FOIA instead of the discovery mechanism provided by the Federal Rules of Civil Procedure. H.R. 1497, 89th Cong., 2d Sess. 11 (1966). When the FOIA was amended in 1974 . . . congressmen were careful to state that they did not desire to permit increased access to investigation files in lieu of discovery.

Id. at 1380, n. 81 (quoting 120 CONG. REC. 17033 (1974)(statement of Sen. Hart)).

217. HEW REPORT, *supra* note 36, at 25-26. (statement of A. Miller, professor of law, Univ. of Michigan).

218. *See* Chrysler Corp. v. Brown, 441 U.S. 281, 294 (1979) (holding that a party submitting documents to a federal agency does not have the right to enjoin their disclosure).

219. HEW REPORT, *supra* note 36, at 35.

220. 44 U.S.C. §§ 3501-3511 (1976).

221. HEW REPORT, *supra* note 36, at 35.

222. *Id.*

223. Freedman, *supra* note 216, at 1398-99.

ment.[224] The crossroads of two trends—more automated information systems and more attention to the individual's privacy rights represent a great challenge. Neither the legal, nor the technological community has handled the conflict adequately. The privacy problem today has economic, political, regulatory, domestic, and international dimensions, as well as technological and legal dimensions.[225]

The Computer Industry Association has voiced concern that the technological development of secure data processing systems represents a complex and extensive undertaking which is not feasible for most manufacturers.[226] One suggestion is that consideration should be given to the creation of a federally chartered non-profit "Super Underwriters Laboratory," which would be responsible for developing technological solutions to the data security problem.[227]

Most approaches to providing technological safeguards include controlling access to the systems based on the principle of isolation.[228] Mechanisms are provided for isolating data and cannot be bypassed by the users of the system.[229] In conjunction with this approach, mechanisms for identifying users and authorizing their access to the system must be developed.[230]

"An effective security system must include the total environment: physical and procedural safeguards as well as those provided by hardware and software."[231] Three goals encompassed by technical security include: (1) Protection of data against physical mishaps, such as fire, flood, theft, or destruction; (2) controlled access to the system by authorized personnel; and (3) integrity of the system—the system performs in accordance with specifications and there are appropriate checks on the accuracy of its data.[232]

General guidelines for the design of hardware to eliminate potential data security problems can never replace continuous review of each product, because one can never predict all the problems which may occur.[233] Even if the system is adequately designed, there is always the possibility that a leak may occur through an error in its im-

---

224. Davis, *A Technologist's View of Privacy and Security in Automated Information Systems*, 4 RUTGERS J. COMPUTER L. 264 (1974).

225. *Id.* at 265.

226. PRIVACY AND SECURITY IN COMPUTER SYSTEMS, *supra* note 11, at IX.

227. *Id.* Data security includes the protection of all files.

228. *Id.*

229. *Id.*

230. *Id.* at X.

231. *Id.*

232. *Id.*

233. *Id.*

plementation.[234] Additionally, there is the problem of remote users. There may be many terminals connected simultaneously and access is often by means of a video screen or keyboard printer terminal. Three potential dangers identified by Professor Barron are: (1) impersonation caused by people masquerading as others entitled to the information; (2) accidental leakage of information caused by a malfunction of the system; and (3) wire-tapping.[235]

Although the demand for data security is growing, customers still rank computer security features below other considerations, such as price, performance, and other special capabilities. Perhaps the following is the most pragmatic definition of security: "a system is secure when the cost of obtaining illicit access to the information exceeds the value of the information so obtained."[236] Anyone with enough money can compile a detailed individual dossier, even from the sources of a decentralized manual filing system. At one time, the high cost of such a project effectively eliminated those with only a casual curiosity in the information from undertaking it. With the advancement of technology, however, this is no longer true.[237]

Professor Barron states that, "contrary to popular opinion, the computer *per se* is not a major threat to society."[238] The technology exists to make computerized databanks secure. It is rarely used at present, however, because it is not generally understood within the computer industry, and because it is very expensive.[239]

Technological security must be purchased and so far there has been no profit motive in the industry to provide security systems. As the computer is used more in privacy sensitive areas, the industry should be forced to realize that it is marketing a potentially dangerous product and like the automobile manufacturer the industry should be expected to take the responsibility for providing the necessary safety features.[240]

V. CONCLUSION

Patchwork legislation and confusion will persist in America until a

234. D.W. BARRON, PRIVACY, PEOPLE NOT COMPUTERS 319, 323 (1978).

235. *Id.* at 325-26.

236. *Id.* at 328.

237. *The Computerization of Government Files, What Impact on the Individual?* 15 UCLA L. REV. 1371 (1968).

238. BARRON, *supra* note 234, at 319.

239. *Id.*

240. Washburn, *supra* note 175, at 208 (quoting Meldman, *Centralized Information Systems and the Legal Right to Privacy*, 4 COMPUTER L. SERV. 5-2 art. 2 at 6 (1969)).

> national privacy policy is established and consistent guidelines formulated that apply to all segments of society. . . . Personal privacy can no longer exist by yesterday's standards.[241]

Many Americans now agree with Professor Linowes. A Harris survey indicated that public concern over privacy and the abuse or misuse of personal information by business and government has increased steadily throughout the Seventies.[242] "In a very real sense, computers are at the heart of the concerns over the loss or potential loss of privacy of personal data."[243]

Minor differences notwithstanding, "there is nothing peculiarly American about the feeling that the struggle of the individual versus computer is a fixed feature of modern life."[244] The problems are universal: loss of individuality and control; creation of dossiers; and centralized bureaucracies.[245]

In a world shrinking due to technological advances, domestic law is not the only answer. International law is necessary. It is interesting to note that European data protection laws were originally privacy protection laws. Europeans are now concerned with how much, not if, protection should be afforded.[246] One must see the whole picture; computerized informational privacy is part of the right to privacy generally and this is a basic human right which must be protected by concerted efforts by organized society throughout the world.[247]

A. *The Patient's Progress Toward Recovery of His Privacy*

Federal legislation is necessary to provide safeguards for privacy. However, it is also necessary for the states to enact appropriate legislation. One state, California, enacted the Confidentiality of Medical Information Act, effective January 1, 1982.[248] The Act limits the circumstances under which an individual's medical records can be

---

241. Linowes, *supra* note 32, at 1184.

242. L. HARRIS & A. WESTIN, THE DIMENSIONS OF PRIVACY, A National Opinion Research Survey of Attitudes Toward Privacy (1981).

243. *Id.* at 76. In the survey the following were cited as the five biggest invaders of privacy from the private sector: finance companies (45%); credit bureaus (44%); insurance companies (38%); credit card companies (37%); newspapers, magazines and television (31%). From the public sector, Americans feel the biggest privacy invaders are: Internal Revenue Service (38%); CIA (34%); FBI (33%); Government welfare agencies (32%); Census Bureau (24%). *Id.*

244. HEW REPORT, *supra* note 36, at 167.

245. *Id.*

246. Evans, *European Data Protection Law*, 29 AM. J. COMP. L. 571, 574 (1981).

247. Freedman, *supra* note 216, at 1398-99.

248. Cal. Civ. Code § 56 (West 1982). *See* Plishner, *supra* note 5, at 251.

disclosed. It covers all health care records, although it does allow for certain limited uses of that information. Medical information cannot be disclosed without the patient's written authorization, except between health care providers for the purpose of diagnosis or treatment.[249]

The Act does not address the patient's right of access to personal medical records, but another law passed in 1982 does. Except for limited situations dealing with mental health records, each individual has the right of access to complete information regarding his condition and the care provided to him.[250]

To accommodate the competing considerations in computerized medical records it may be helpful to recognize that most of the advantages achieved by the compilation of statistical data could be achieved without the recording of personally identifiable information. Such bifurcation should be considered in the initial transfer of information to the computer. Further, patients should be informed if the information supplied may be subsequently released to third parties, and of the possible consequences of disclosure. Additionally, written consent should be obtained from the patient before any information is disclosed.[251] Legislative support prohibiting certain types of requests or adequate warnings regarding disclosure might be appropriate. To help guard against inaccurate information, patients upon request should be permitted to inspect their own files. Further, there should be definite time limits for keeping "stale" information. This is particularly necessary in cases in which a patient has left psychiatric or mental health therapy. The stigma on the individual far outweighs the necessity for keeping the information indefinitely.

Centralized health computer systems are both a promise and a threat. Used correctly the benefits could be maximized and the dangers minimized.[252]

B. *Alternative Treatment Plans: Personal Privacy*

Some commentators have advocated an amendment to the Federal Constitution to clearly and unequivocally establish the right to personal privacy. At least three state constitutions have a specific right of privacy—California,[253] Alaska,[254] and South Carolina.[255]

249. Pilsner, *supra* note 5, at 251.
250. CAL. HEALTH AND SAFETY CODE §§ 25250-58 (West 1982).
251. *See supra* notes 76-79 and accompanying text.
252. Gobert, *supra* note 2, at 186-87.
253. CAL. CONST. art. I, § 1 (West 1982).
254. ALASKA CONST. art. I, § 22 (1980).

Where disclosure of personal information is not clearly proscribed by statute, a constitutional right to privacy would put any organization making such a disclosure at the peril of being a defendant in a potential law suit.

Another suggestion is to extend tort liability to the computer information processor. The processor would be liable for any breach of due care, which would include reasonable inquiry and be judged against standards of an ordinarily prudent person within the industry and under similar circumstances. Further, consideration should be given to eliminating the requirement of proof as to actual damages.[256]

Other suggestions to protect privacy include the appointment of an ombudsman to supervise data systems, or the creation of a federal regulatory agency to control all computerized data systems.

Some commentators have urged that control provisions be tailored to the nature of the data systems, with separate legislation for computerized medical systems, criminal justice systems, and credit reporting organizations. Westin and Baker state:

> [I]t appears clear to us that no single law, constitutional amendment, or court decision can cope with the tremendous diversity of issues and settings, and the uneven readiness for corrective action, that make up the current data-bank problem. Such total solutions are not worth pursuing.[257]

There are no easy solutions. The ultimate answer lies with the public. Politics and policy will ultimately dictate future action or inaction. In conclusion, it is important to maintain the following goals in the area of privacy:

1. There should be some legitimate purpose for the collection of information;
2. An organization should not transfer information to a third-party without the subject's consent;
3. An individual should have notice that information is being collected, who will get the information, and how it will be used;
4. No information should be obtained under false pretenses;
5. The individual should have the continuing right to see and copy records about himself that any organization has on file;
6. If the accuracy of information is questioned, the individual should have the right to correct the record;

---

255. S.C. CONST. art. I, § 9 (1977).

256. G. Stevens, H. Hoffman, *Tort Liability for Defamation by Computer*, 6 J. OF COMPUTERS AND L. 91, 102 (1977).

257. A. WESTIN & M. BAKER, *supra* note 64, at 350-51.

7. If the statement is in dispute, a permanent copy of the statement of the individual's position should be attached to the record;
8. Disclosure should be made only to authorized parties and only after consent by the individual has been freely given;
9. The retention of information should have a time limit and material no longer useful for the particular purpose for which it was collected should be destroyed; and
10. There should be an administrative procedure for resolving disputes.

It is not technology as such, which affects society for good or bad, but its uses, which are, in form, shaped by the values of society and by the historical context in which the technology is used. . . . We must remember that we are not trapped helplessly in front of an unstoppable technological steamroller. Our control is how we use our knowledge that we will be required to live with the results of our decisions on the use of this new technology.[258]

258. F. Weingarten, *Privacy: A Terminal Idea*, 10 HUM. RTS. J. 56 (1982).